



1925 Vaughn Road, Suite 215  
Kennesaw, Georgia 30144  
+1.678.460.1475

To: Commission's Secretary  
Office of the Secretary  
Federal Communications Commission  
445 12th Street, SW, Suite TW-A325  
Washington, DC 20554

From: IP Communications, LLC.  
FRN: 0014-0615-19  
Filing Date: February 13, 2019  
RE: Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

I, James M. Doneghy, Jr., certify that I am the Chief Executive Officer of IP Communications, LLC. and, acting as an agent of the company, I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules.

IP Communications has not taken any actions against data brokers in the past year. We have not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Attached to this certification is an accompanying statement explaining how IP Communications' procedures ensure it is in compliance with the requirements set forth in section the Commission's rules regarding CPNI information.

Signed

A handwritten signature in black ink, appearing to read "J. Doneghy", written over a horizontal line.

James M. Doneghy, Jr.  
Chief Executive Officer  
IP Communications, LLC.  
February 13, 2019

To: Commission's Secretary



1925 Vaughn Road, Suite 215  
Kennesaw, Georgia 30144  
+1.678.460.1475

Office of the Secretary  
Federal Communications Commission  
445 12th Street, SW, Suite TW-A325  
Washington, DC 20554

From: IP Communications, LLC.  
FRN: 0014-0615-19  
Feb, 13, 2019

RE: Accompanying Statement to Annual CPNI Compliance Certificate (Reference: EB Docket No. 06)

IP Communications has set forth the following rules and procedures regarding the safe-keeping of its customer's information:

Employee Training – All employees must review the procedures and processes in regards to the safe keeping of CPNI. IP Communications also holds annual training sessions about CPNI processes and procedures. All new employees are trained on CPNI procedures before they begin working.

Customer Authentication - Since the release of call detail information over the telephone presents an immediate risk to our customer's privacy, all employees of IP Communications are prohibited from releasing call detail information based on customer-initiated telephone contact, except under three circumstances: (1) when an IP Communications customer provides a pre-established verbal or online password; (2) when an IP Communications customer requests that the information be sent to (and only to) the customer's billing address on file; or (3) when an IP Communications employee initiates a call to the telephone number on record and discloses the information.

Password Protection - IP Communications provides mandatory password protection for online account access to our web based account management interface. Online access based solely on a customer's readily available biographical information is prohibited, and our system is programmed and must remain programmed such that it will only accept passwords that meet our specific password requirements and restrictions that ensure that only highly unique and secure passwords are utilized by our customers to access our online systems.

Network and PC Protection - IP Communications requires that all of its personal computers and servers that might come in contact with CPNI have (at minimum) software based firewalls, antivirus protection and where necessary file encryption applications. Under no circumstance is CPNI data to be emailed across the public internet.

Notice of Account Changes – IP Communications has processes in place to notify our customer immediately of account activity, such as a change to a password, an online account or an address of record. When this occurs online, our system will automatically send a notification to the address on file that a change has occurred on their account. When a change is requested by phone (after verification of verbal or online password our processes ensure that we follow the phone conversation with a notification to the address on file that a change has occurred on their account.

In the event of Unauthorized Disclosure of CPNI - If for any reason there has been a breach of CPNI, or if an IP Communications employee has reason to believe that CPNI information may have been disseminated to an unauthorized recipient, that employees must notify a senior member of management immediately. The CEO or President of IP Communications will provide electronic notification of the breach within seven business days to the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI"). The CEO or President of IP Communications will then wait another seven business days before notifying the affected customers of the breach (unless the USSS and FBI request that the carrier continue to postpone disclosure). However, the CEO or President of IP Communications may notify customers sooner if there is a risk of immediate and irreparable harm.

Record Keeping - IP Communications has processes in place to ensure that all we keep records of discovered breaches for at least seven years. These records will be stored electronically in our secure network drives and a paper copy will be stored and locked in an on-premise secure file cabinet reserved for such information.

Failure to Comply with CPNI Processes or Procedures: If any employee fails to comply with any of the procedures or processes regarding the safe keeping of CPNI, they have been made aware that they will be subject to disciplinary actions that ultimately may require employment termination.